WHAT IS CLAIMED IS:

1. A data processing apparatus for performing rights processing of content data encrypted with content key data based on usage control policy data, and for decrypting the encrypted content key data, said data processing apparatus comprising within a tamper-resistant circuit module:

a first bus;

an arithmetic processing circuit connected to said first bus, for performing the rights processing of the content data based on the usage control policy data;

a storage circuit connected to said first bus;

a second bus;

a first interface circuit interposed between said first bus and said second bus;

an encryption processing circuit connected to said second bus, for decrypting the content key data; and

an external bus interface circuit connected to said second bus.

2. A data processing apparatus according to claim 1, further comprising a second interface circuit within said tamper-resistant circuit module, wherein said first bus comprises a third bus connected to said arithmetic processing circuit and said storage circuit, and a fourth

bus connected to said first interface circuit, and said second interface circuit is interposed between said third bus and said fourth bus.

3. A data processing apparatus according to claim 2, further comprising within said tamper-resistant circuit module:

a fifth bus;

a third interface circuit connected to said fifth bus, for performing communication with a data processing circuit having an authentication function which is loaded on one of a recording medium and an integrated circuit card; and

a fourth interface circuit interposed between said fourth bus and said fifth bus.

4. A data processing apparatus according to claim 1, wherein said encryption processing circuit comprises a public-key encryption circuit and a common-key encryption circuit.

5. A data processing apparatus according to claim 4, wherein:

said storage circuit stores private key data of said data processing apparatus and public key data of a second data processing apparatus;

said public-key encryption circuit verifies the integrity of signature data, which verifies the integrity of the content data, the content key data, and the usage control policy data, by using the corresponding public key data, and when recording the content data, the content key data, and the usage control policy data on a recording medium or when sending them to said second data processing apparatus, said public-key encryption circuit creates signature data, which verifies the integrity of the content data, the content key data, and the usage control policy data, by using the private key data; and

said common-key encryption circuit decrypts the content key data, and when sending the content data, the content key data, and the usage control policy data to said second data processing apparatus online, said common-key encryption circuit encrypts and decrypts the content data, the content key data, and the usage control policy data by using session key data obtained by performing mutual authentication with said second data processing apparatus.

6. A data processing apparatus according to claim 5, further comprising a hash-value generating circuit within said tamper-resistant circuit module, for generating hash values of the content data, the content key data and the usage control policy data, wherein said public-key

encryption circuit verifies the integrity of the signature data and creates the signature data by using the hash values.

7. A data processing apparatus according to claim 1, further comprising a random-number generating circuit within said tamper-resistant circuit module, said random-number generating circuit being connected to said second bus, for generating a random number for performing mutual authentication with said second data processing apparatus when sending the content data, the content key data, and the usage control policy data to said second data processing apparatus online.

8. A data processing apparatus according to claim 1, wherein said external bus interface circuit is connected to an external storage circuit for storing at least one of the content data, the content key data, and the usage control policy data.

9. A data processing apparatus according to claim 8, further comprising a storage-circuit control circuit for controlling access to said storage circuit and access to said external storage circuit via said external bus interface circuit in accordance with a command from said arithmetic processing circuit.

10. A data processing apparatus according to claim 1, wherein said external bus interface circuit is connected to a host arithmetic processing apparatus for centrally controlling a system on which said data processing apparatus is loaded.

11. A data processing apparatus according to claim 8, further comprising a storage management circuit for managing an address space of said storage circuit and an address space of said external storage circuit.

12. A data processing apparatus according to claim 1, wherein said arithmetic processing circuit determines at least one of a purchase mode and a usage mode of the content data based on a handling policy indicated by the usage control policy data, and creates log data indicating a result of the determined mode.

13. A data processing apparatus according to claim 12, wherein, after determining the purchase mode, said arithmetic processing circuit creates usage control status data in accordance with the determined purchase mode, and controls the use of the content data based on the usage control status data.

14. A data processing apparatus according to claim 4, wherein, in recording the content data, for which the purchase mode is determined, on a recording medium, said common-key encryption circuit encrypts the content key data and the usage control status data by using medium key data corresponding to said recording medium.

15. A data processing apparatus according to claim 4, wherein, when the content key data is encrypted with license key data having an effective period, said storage circuit stores the license key data, said data processing apparatus further comprises a real time clock for generating real time, said arithmetic processing circuit reads the effective license key data from said storage circuit based on the real time indicated by said real time clock, and said common-key encryption circuit decrypts the content key data by using the read license key data.

16. A data processing apparatus according to claim 1, wherein said storage circuit writes and erases data in units of blocks, and said data processing apparatus comprises within said tamper-resistant circuit module, a write-lock control circuit for controlling the writing and erasing of the data into and from said storage circuit in units of

blocks under the control of said arithmetic processing circuit.

17. A data processing apparatus for performing rights processing of content data encrypted with content key data based on usage control policy data, and for decrypting the encrypted content key data, said data processing apparatus comprising within a tamper-resistant circuit module:

a first bus;

an arithmetic processing circuit connected to said first bus, for performing the rights processing of the content data based on the usage control policy data;

a storage circuit connected to said first bus;

a second bus;

an interface circuit interposed between said first bus and said second bus;

an encryption processing circuit connected to said second bus, for decrypting the content key data; and

an external bus interface circuit connected to said second bus,

wherein, upon receiving an interrupt from an external circuit via said external bus interface circuit, said arithmetic processing circuit becomes a slave for said external circuit so as to perform processing designated by the interrupt, and reports a result of the processing to

said external circuit.

18. A data processing apparatus according to claim 17, wherein said arithmetic processing circuit reports the result of the processing by outputting an interrupt to said external circuit.

19. A data processing apparatus according to claim 17, wherein said external bus interface comprises a common memory for said arithmetic processing circuit and said external circuit, and said arithmetic processing circuit writes the result of the processing into said common memory, and said external circuit obtains the result of the processing by polling.

20. A data processing apparatus according to claim 19, wherein said external bus interface comprises:

a first status register indicating an execution status of the processing requested from said external circuit in said arithmetic processing circuit, and including a flag set by said arithmetic processing circuit and read by said external circuit;

a second status register indicating whether said external circuit has requested said arithmetic processing circuit to perform processing, and including a flag set by

said external circuit and read by said arithmetic processing circuit; and

said common memory for storing a result of the processing.

21. A data processing apparatus according to claim 18, wherein said storage circuit stores an interrupt program describing the processing designated by the interrupt, and said arithmetic processing circuit performs the processing by executing the interrupt program read from said storage circuit.

22. A data processing apparatus according to claim 21, wherein said storage circuit stores a plurality of said interrupt programs, and a plurality of sub-routines to be read when executing the interrupt program, and said arithmetic processing circuit appropriately reads and executes the sub-routines from said storage circuit when executing the interrupt program read from said storage circuit.

23. A data processing system comprising:

an arithmetic processing apparatus, for executing a predetermined program and for outputting an interrupt according to a predetermined condition by serving as a

master; and

a data processing apparatus, for performing predetermined processing in response to the interrupt from said arithmetic processing apparatus by serving as a slave for said arithmetic processing apparatus, and for reporting a result of the processing to said arithmetic processing apparatus, said data processing apparatus comprising within a tamper-resistant circuit module:

determining means for determining at least one of a purchase mode and a usage mode of content data based on a handling policy indicated by usage control policy data;

log data generating means for generating log data indicating a result of the determined mode; and

decrypting means for decrypting the content key data.

24. A data processing system according to claim 23, wherein, upon receiving the interrupt indicating an interrupt type, said arithmetic processing apparatus outputs to said data processing apparatus an interrupt indicating an instruction to execute an interrupt routine corresponding to the interrupt type, and said data processing apparatus executes the interrupt routine corresponding to the interrupt type of the interrupt received from said arithmetic processing apparatus.

25. A data processing system according to claim 23, wherein said data processing apparatus reports a result of the processing by outputting an interrupt to said arithmetic processing apparatus.

26. A data processing system according to claim 23, wherein said data processing apparatus comprises a common memory which is accessible by said data processing apparatus and said arithmetic processing apparatus, and said arithmetic processing apparatus obtains the result of the processing by accessing said common memory through polling.

27. A data processing system according to claim 26, wherein said data processing apparatus comprises a first status register indicating an execution status of the processing requested from said arithmetic processing apparatus, and including a flag read by said arithmetic processing apparatus;

a second status register indicating whether said arithmetic processing apparatus has requested said data processing apparatus to perform processing by the interrupt, and including a flag set by said arithmetic processing apparatus; and

said common memory for storing a result of the processing.

28. A data processing system according to claim 23, further comprising a bus for connecting said arithmetic processing apparatus and said data processing apparatus.

29. A data processing system according to claim 24, wherein said data processing apparatus enters a low power state after completing the execution of one of an initial program and the interrupt routine.

30. A data processing system according to claim 24, wherein, based on the interrupt received from said arithmetic processing apparatus, said data processing apparatus executes the interrupt routine in accordance with at least one of processing for determining one of the purchase mode and the usage mode of the content data, processing for reproducing the content data, and processing for downloading the data from a certifying authority.

31. A data processing system according to claim 23, wherein said arithmetic processing apparatus executes a predetermined user program.

32. A data processing system in which content data provided by a data providing apparatus is received from a

data distribution apparatus, and is managed by a management apparatus, said data processing system comprising:

a first processing module for receiving from said data distribution apparatus a module in which content data encrypted with content key data, the encrypted content key data, usage control policy data indicating a handling policy of the content data, and price data for the content data determined by said data distribution apparatus are stored, and for decrypting the received module by using common key data, and for performing accounting processing for a distribution service of the module by said data distribution apparatus;

an arithmetic processing apparatus for executing a predetermined program and for outputting an interrupt according to a predetermined condition by serving as a master; and

a data processing apparatus for performing predetermined processing in response to the interrupt from said arithmetic processing apparatus by serving as a slave for said arithmetic processing apparatus, and for reporting a result of the processing to said arithmetic processing apparatus, said data processing apparatus comprising within a tamper-resistant circuit module:

determining means for determining at least one of a purchase mode and a usage mode of the content data based on

the handling policy indicated by the usage control policy data stored in the received module;

log data generating means for generating log data indicating a result of the determined mode;

output means for outputting the price data and the log data to said management apparatus when the purchase mode of the content data is determined; and

decrypting means for decrypting the content key data.

33. A data processing system comprising:

an arithmetic processing apparatus for executing a predetermined program and for outputting an interrupt according to a predetermined condition by serving as a master;

a first tamper-resistant data processing apparatus for performing rights processing of content data encrypted with content key data in response to the interrupt from said arithmetic processing apparatus by serving as a slave for said arithmetic processing apparatus, and for reporting a result of the processing to said arithmetic processing apparatus; and

a second tamper-resistant data processing apparatus for decrypting the content data by using the content key data obtained by performing mutual authentication with said first

tamper-resistant data processing apparatus and for compressing or decompressing the content data in response to the interrupt from said arithmetic processing apparatus or said first tamper-resistant data processing apparatus by serving as a slave for said arithmetic processing apparatus or said first tamper-resistant data processing apparatus.

34. A data processing system according to claim 33, further comprising a bus for connecting said arithmetic processing apparatus, said first tamper-resistant data processing apparatus, and said second tamper-resistant data processing apparatus.

35. A data processing system comprising:

an arithmetic processing apparatus for executing a predetermined program and for outputting an interrupt according to a predetermined condition by serving as a master;

a first tamper-resistant data processing apparatus for performing rights processing of content data encrypted with content key data in response to the interrupt from said arithmetic processing apparatus by serving as a slave for said arithmetic processing apparatus, and for reporting a result of the processing to said arithmetic processing apparatus; and

a second tamper-resistant data processing apparatus for performing mutual authentication with said arithmetic processing apparatus and for reading and writing the content data from and into a recording medium in response to the interrupt output from said arithmetic processing apparatus.

36. A data processing system according to claim 35, wherein said second tamper-resistant processing apparatus decrypts and encrypts the content data by using medium key data corresponding to said recording medium.

37. A data processing system according to claim 35, wherein, when said recording medium is provided with a processing circuit having a mutual authentication function, said second tamper-resistant processing apparatus performs mutual authentication with said processing circuit.

38. A data processing system comprising:

an arithmetic processing apparatus for executing a predetermined program and for outputting an interrupt according to a predetermined condition by serving as a master;

a first tamper-resistant data processing apparatus for performing mutual authentication with said arithmetic processing apparatus and for reading and writing content

data from and into a recording medium in response to the interrupt from said arithmetic processing apparatus; and

a second tamper-resistant data processing apparatus for decrypting the content data by using content key data and for compressing or decompressing the content data in response to the interrupt from said arithmetic processing apparatus by serving as a slave for said arithmetic processing apparatus.

39. A data processing system according to claim 38, further comprising a storage circuit for temporarily storing the content data read from said recording medium by said first tamper-resistant data processing apparatus, and for outputting the stored content data to said second tamper-resistant data processing apparatus.

40. A data processing system according to claim 39, wherein said storage circuit utilizes part of a storage area of an anti-vibration storage circuit.

41. A data processing system according to claim 38, further comprising a third tamper-resistant data processing apparatus for performing rights processing of the content data encrypted with the content key data in response to the interrupt from said arithmetic processing apparatus by

serving as a slave for said arithmetic processing apparatus, and for reporting a result of the processing to said arithmetic processing apparatus.

42. A data processing method using an arithmetic processing apparatus and a data processing apparatus, said data processing method comprising the steps of:

executing, in said arithmetic processing apparatus, a predetermined program and outputting an interrupt according to a predetermined condition by serving as a master; and

determining, in said data processing apparatus, at least one of a purchase mode and a usage mode of content data based on a handling policy of usage control policy data, creating log data indicating a result of the determined mode, and decrypting content key data, within a tamper-resistant circuit module in response to the interrupt from said arithmetic processing apparatus by serving as a slave for said arithmetic processing apparatus.

43. A data processing method according to claim 42, wherein, upon receiving the interrupt indicating an interrupt type, said arithmetic processing apparatus outputs to said data processing apparatus an interrupt indicating an instruction to execute an interrupt routine corresponding to the interrupt type, and said data processing apparatus

executes the interrupt routine corresponding to the processing designated by the interrupt received from said arithmetic processing apparatus.

44. A data processing method according to claim 42, wherein said data processing apparatus reports the result of the processing by outputting an interrupt to said arithmetic processing apparatus.

45. A data processing method according to claim 42, wherein said data processing apparatus comprises a common memory which is accessible by said data processing apparatus and said arithmetic processing apparatus, and said arithmetic processing apparatus obtains the result of the processing by accessing said common memory through polling.

46. A data processing method according to claim 45, wherein:

said data processing apparatus sets a flag in a first status register indicating an execution status of the processing requested by the interrupt from said arithmetic processing apparatus;

said arithmetic processing apparatus reads the execution status of the processing of said data processing apparatus from the flag in said first status register;

said arithmetic processing apparatus sets a flag in a second status register indicating whether said arithmetic processing apparatus has requested said data processing apparatus to perform the processing through the interrupt; and

said data processing apparatus determines whether said arithmetic processing apparatus has requested said data processing apparatus to perform the processing from the flag in said second status register.

47. A data processing method according to claim 42, wherein said data processing apparatus enters a low power state upon completion of the execution of one of an initial program and the interrupt routine.

48. A data processing method according to claim 42, wherein, based on the interrupt received from said arithmetic processing apparatus, said data processing apparatus executes the interrupt routine in accordance with at least one of processing for determining one of the purchase mode and the usage mode of the content data, processing for reproducing the content data, and processing for downloading the data from a certifying authority.

49. A data processing method according to claim 42,

wherein said arithmetic processing apparatus executes a predetermined user program.

50. A data processing method using an arithmetic processing apparatus, a first data processing apparatus, and a second data processing apparatus, said data processing method comprising the steps of:

executing, in said arithmetic processing apparatus, a predetermined program and outputting an interrupt according to a predetermined condition by serving as a master;

performing, in said first data processing apparatus, rights processing of content data encrypted with content key data within a tamper-resistant module in response to the interrupt from said arithmetic processing apparatus by serving as a slave for said arithmetic processing apparatus, and reporting a result of the processing to said arithmetic processing apparatus; and

decrypting, in said second data processing apparatus, the content data by using the content key data obtained by performing mutual authentication with said first data processing apparatus and compressing or decompressing the content data within a tamper-resistant module in response to the interrupt from said arithmetic processing apparatus or said first data processing apparatus by serving as a slave for said arithmetic processing apparatus or said first data

processing apparatus.

51. A data processing method using an arithmetic processing apparatus, a first data processing apparatus, and a second data processing apparatus, said data processing method comprising the steps of:

executing, in said arithmetic processing apparatus, a predetermined program and outputting an interrupt according to a predetermined condition by serving as a master;

performing, in said first data processing apparatus, rights processing of content data encrypted with content key data within a tamper-resistant module in response to the interrupt from said arithmetic processing apparatus by serving as a slave for said arithmetic processing apparatus, and reporting a result of the processing to said arithmetic processing apparatus; and

performing, in said second data processing apparatus, mutual authentication with said arithmetic processing apparatus, and reading and writing the content data from and into a recording medium within a tamper-resistant module in response to the interrupt from said arithmetic processing apparatus.

52. A data processing method according to claim 51, wherein said second data processing apparatus decrypts and

encrypts the content data by using medium key data corresponding to said recording medium.

53. A data processing method according to claim 51, wherein, when said recording medium is provided with a processing circuit having a mutual authentication function, said second data processing apparatus performs mutual authentication with said processing circuit.

54. A data processing method using an arithmetic processing apparatus, a first data processing apparatus, and a second data processing apparatus, said data processing method comprising the steps of:

executing, in said arithmetic processing apparatus, a predetermined program and outputting an interrupt according to a predetermined condition by serving as a master;

performing, in said first data processing apparatus, mutual authentication with said arithmetic processing apparatus, and reading and writing content data from and into a recording medium within a tamper-resistant module in response to the interrupt from said arithmetic processing apparatus; and

decrypting, in said second data processing apparatus, the content data by using content key data and compressing or decompressing the content data within a tamper-resistant

module in response to the interrupt from said arithmetic processing apparatus by serving as a slave for said arithmetic processing apparatus.

55. A data processing method according to claim 54, wherein the content data read from said recording medium by said first data processing apparatus is temporarily stored in a storage circuit, and the content data read from said storage circuit is output to said second data processing apparatus.

56. A data processing method according to claim 55, wherein said storage circuit utilizes part of a storage area of an anti-vibration storage circuit.